EXHIBIT 42

Message

From: Hamilton, Dave [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=955025E6B47A436F84406099716ACBA8-HAMILTON, D]
Sent: 12/21/2020 2:28:11 PM
To: Beaver, Merritt [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=cf9722d544f8476ab2513232dbb6d894-Beaver, Mer]
CC: IT Security [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8c095e7e7aa441ebb405c47b1a93d27c-IT Security]
Subject: Re: The 590 Rule Attestation

Exhibit 0017

We need Civix to produce the reports and information that are required by the rule.

Based on previous years reports I surmise that James hopefully received something, just don't know if he actually requested it, or if he just took their word, but either way, there is no record of it. I eventually went through Calvin, their new CISO, since most of the artifacts he should have at the ready, as I do, if the situation was reversed.

Nick asked Melissa, Sanchin and others over the last month for any of this information to no avail. We finally got more info from Keval of where to look that we did from Civix but we still need the artifact reports. We really just can't just take their word for it. I have a suspicion that they didn't perform a Security Risk Assessment (SRA) this year, or likely the last few years as they are required by the Rule.

Additionally, It seems incredible to me that they cannot provide something as simple as the proof as to what the designed password restriction in eNet is, they can't even point to an original design spec to verify against. That's an example of a significant gap in our assessment.

What I am looking for is something as simple as the standard 8 character, complex, upper,lower one number, not a dictionary word and they force users to change it on some schedule. And that they don't store these passwords in clear text in the database and they encrypt or hash them. But I need something to document it, not just a statement in an email, show me the code snippet, the XML settings, etc.

Something mirroring the basic Microsoft standards would be a good place to start. But these are the guys that whipped up their own MFA solution rather than bolting on something commercial and widely proven as secure and resilient.

On our part, we did everything we could to meet these rules. The guys all busted it and dig deep to produce credible, repeatable artifact examples that confirm what we know to be true. A significant portion of the partials can be remediated once we get eNet moved over to the new environment. My plan was to produce an amendment shortly after the first of the year, once eNet lands and I can verify the risk gaps are minimized. Too late for this years attestation but might help if we can show progress even though it's late, we can blame COVID.

I documented in the Next Steps section on each item what we can do to close the gap.

The largest impact can be made by getting Civix to produce their part of this. We can go from 66% up to over 80% quickly.

I'm not familiar with the process of endorsement, if it's a binary pass/fail and we're done until next year, or there is a defined "cure" period that we might be able to use to close these gaps.

The last commitment I received from Civix was by COB on 26 December. I sent them the actual language from the Rule so there was no misunderstanding. We will see how they do.

Dave

David Hamilton – CISSP, C|CISO, CISM, CDPSE, CRISC, HCISPP
Chief Information Security Officer
Office of Georgia Secretary of State
2 Martin Luther King Jr. Dr. SE,
Atlanta, GA 30334
P: 470.312.2649
C:404-229-7830
dhamilton@sos.ga.gov

From: Beaver, Merritt <mbeaver@sos.ga.gov>
Sent: Monday, December 21, 2020 8:48:53 AM
To: Hamilton, Dave <dhamilton@sos.ga.gov>
Subject: RE: The 590 Rule Attestation

Are in compliance or do we need to do anything at this time

S. Merritt Beaver
Chief Information Officer
Georgia Secretary of State
Office (470) 312-2727 Mobile: (770)330-0016
mbeaver@sos.ga.gov

From: Hamilton, Dave <dhamilton@sos.ga.gov>
Sent: Saturday, December 19, 2020 8:15 PM
To: Beaver, Merritt <mbeaver@sos.ga.gov>
Cc: IT Security <itsecurity@sos.ga.gov>
Subject: Re: The 590 Rule Attestation

Not sure why it didn't send the first time – here you go.

From: David Hamilton <dhamilton@sos.ga.gov>
Date: Saturday, December 19, 2020 at 4:14 PM
To: "Beaver, Merritt" <mbeaver@sos.ga.gov>
Cc: IT Security <itsecurity@sos.ga.gov>
Subject: The 590 Rule Attestation

Merritt,

This took a lot longer than we first thought, I really don't understand how my predecessor was ever able to attest to meeting this set of regulations. I handled this just like an assessment, if we cant come up with an artifact that proves something is real – it doesn't exist. The guys on the Security team and I worked tirelessly on capturing these artifacts, and it will be much easier next year.

Civix was basically unresponsive until we beat them up – and we still don't have anything, Calvin's commitment was COB on 12/26. Not holding my breath, I don't think they did a Risk Assessment this year.

This is a DRAFT, you can let me know what does and doesn't get forwarded to Ryan and/or Brad, understanding it's lilely a single page signed that we either did or didn't meet the Rule, since he is ultimately on the hook for the accuracy.

Dave

David Hamilton – CISSP, C|CISO, CISM, CDPSE, CRISC, HCISPP
Chief Information Security Officer
Office of Georgia Secretary of State
2 Martin Luther King Jr. Dr. SE,
Atlanta, GA 30334
P: 470.312.2649
C:404-229-7830
dhamilton@sos.ga.gov